UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

CANDICE FACON and BENJAMIN KASHVILI, on behalf of themselves individually and on behalf of all others similarly situated, Plaintiff, v. M&D CAPITAL PREMIER BILLING LLC, Defendant.	**CASE NO. 24-cv-2374** **CLASS ACTION COMPLAINT** **JURY DEMAND**

CLASS ACTION COMPLAINT

Plaintiffs CANDICE FACON and BENJAMIN KASHVILI ("Plaintiff") bring this Class Action Complaint ("Complaint") against Defendant M&D CAPITAL PREMIER BILLING LLC ("M&D" or "Defendant") as individuals and on behalf of all others similarly situated, and alleges, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data Breach").

2. The Data Breach resulted in the unauthorized disclosure, exfiltration, and theft of consumers' highly personal information, including names, dates of birth, insurance information Social Security number, financial information, ("personal identifying information" or "PII"), medical billing information and certain medical information including diagnoses, medication, and

treatment information ("protected health information" or "PHI"). Plaintiffs refer to both PII and PHI collectively as "Sensitive Information."

3. M&D's breach differs from typical data breaches because it affects consumers who had no relationship with M&D, never sought one, and never consented to M&D collecting and storing their information.

4. On information and belief, the Data Breach occurred between June 20, 2023, and July 8, 2023. M&D did not become aware of suspicious activity on its network until July 8, 2023, an appalling eighteen days after the Data Breach had first begun.

5. On March 18, 2024, M&D finally notified state Attorneys General and many putative Class Members about the widespread Data Breach ("Notice Letter"). A Sample Notice Letter is attached as **Exhibit A**. Plaintiff Faco's Notice Letter is attached as **Exhibit B.** M&D waited over eight months before informing Class Members about the Data Breach, even though Plaintiffs and thousands of Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

6. M&D's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its consumers how many people were impacted, how the breach happened on M&D's systems, or why it took M&D over eight months to begin notifying victims that hackers had gained access to highly private Sensitive Information.

7. Defendant's failure to timely detect and report the Data Breach made its consumers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

8. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII and PHI misuse.

9. In failing to adequately protect Plaintiffs' and the Class's Sensitive Information, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed an unknown number of its current and former consumers.

10. Plaintiffs and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiffs and members of the proposed Class trusted Defendant with their Sensitive Information. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiffs are Data Breach victims.

12. Accordingly, Plaintiffs, on their own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

13. Plaintiff, Candice Facon, is a natural person and citizen of New Jersey, where she intends to remain.

14. Plaintiff, Benjamin Kashvili, is a natural person and citizen of New York, where he intends to remain.

15. Defendant, M&D, is a New York limited liability company with its principal place of business at 115-06 Myrtle Ave, Richmond Hill, New York 11418.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class. At least one Plaintiff and Defendant are citizens of different states.

17. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and does substantial business in this District.

18. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

STATEMENT OF FACTS

M&D

19. M&D is a medical billing service that has "deep experience in managing the complicated financial affairs of medical practices" and specializes in "helping practices with financial challenges realize significant gains in revenue." M&D touts some of its core values to be "transparency", "quality", and "stability", boasting that "with years in the healthcare billing industry, M&D makes a trustworthy partner for your practice or surgical center."[1] M&D boasts a total annual revenue of more than $5 million.[2]

20. As it itself recognizes, M&D's software services are specialized for healthcare providers who oversee highly sensitive data. M&D thus must oversee, manage, and protect the Sensitive Information of its clients' patients, M&D's consumers.

[1] About us, MD, https://mdcapitalbilling.com/about-us/ (last visited March 28, 2024).
[2] MD, Zoominfo, https://www.zoominfo.com/c/m-d-medical-billing/513013036 (last visited March 28, 2024).

21. On information and belief, these third-party consumers, whose Sensitive Information was collected by M&D, do not directly do any business with M&D.

22. As a self-proclaimed leader in its industry handling highly sensitive aspects of its clients' business, M&D understood the need to protect its client's patient's data and prioritize its data security.

23. Indeed, M&D boasts on its website that it "maintain[s] full HIPAA compliancy."[3]

24. Despite recognizing its duty to do so, on information and belief, M&D has not implemented reasonably cybersecurity safeguards or policies to protect its consumers' Sensitive Information or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, M&D leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' Sensitive Information.

The Data Breach

25. Plaintiff Facon is unsure how M&D got her information but assumes her healthcare provider, Premier Anesthesia Associates, provided M&D with her Sensitive Information, including but not limited to her name, address, medical billing and insurance information, certain medical information including diagnoses, medication and treatments, date of birth, Social Security number, and financial information.

26. Plaintiff Kashvili is unsure how M&D got his information but assumes his healthcare provider provided M&D with his Sensitive Information, including but not limited to his name, date of birth, social security number, financial information, medical information, medical billing information, and insurance information.

[3]Technology, M&D, https://mdcapitalbilling.com/technology/ (last visited March 28, 2024).

27. On information and belief, Defendant collects and maintains consumers' Sensitive Information in its computer systems.

28. In collecting and maintaining Sensitive Information, Defendant implicitly agrees that it will safeguard the data using reasonable means according to its internal policies, as well as state and federal law.

29. According to the Breach Notice, on July 8, 2023, M&D "identified suspicious activity within our computer environment." Ex. A. Following an internal investigation, M&D admitted that "an unauthorized threat actor may have had access to certain systems beginning on or around June 20, 2023" and that as a result, "certain files within our systems may have been accessed or acquired by the unauthorized threat actor." Ex. A.

30. In other words, M&D's investigation revealed that its network had been hacked by cybercriminals at least eighteen days before notice and that Defendant's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its consumers' highly private Sensitive Information.

31. Through its inadequate security practices, Defendant exposed Plaintiffs' and the Class's Sensitive Information for theft and sale on the dark web.

32. On or around March 18, 2024 –over eight months after the Breach first occurred – M&D finally notified Plaintiffs and Class Members about the Data Breach.

33. Despite its duties and alleged commitments to safeguard Sensitive Information, Defendant did not in fact follow industry standard practices in securing consumers' Sensitive Information, as evidenced by the Data Breach.

34. In response to the Data Breach, Defendant contends that it has or will be "further enhance[ing] the security of our systems" and has "implemented additional administrative and

technical safeguards" Ex. A. Although Defendant fails to expand on what these alleged "enhancements" and "additional safeguards" are, such steps should have been in place before the Data Breach.

35. Through the Data Breach, Defendant recognized its duty to implement reasonable cybersecurity safeguards or policies to protect consumers' Sensitive Information, insisting that, despite the Data Breach demonstrating otherwise, Defendant "take[s] the confidentiality, privacy, and security of information in our possession seriously" further stating that "we value your privacy and sincerely regret any inconvenience this matter may cause. Your confidence in our ability to safeguard your personal information and your peace of mind are very important to us." Ex. A.

36. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant and to continually review your healthcare insurance information [,] credit report, bank account activity, and bank statements for irregularities or unauthorized items, and to immediately report any unauthorized charges to your financial institution." Ex. A.

37. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiffs' and the Class's Sensitive Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

38. On information and belief, M&D has offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves Sensitive Information that cannot be changed, such as Social Security numbers.

39. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' Sensitive Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

40. Because of the Data Breach, Defendant inflicted injuries upon Plaintiffs and Class Members. And yet, Defendant has done absolutely nothing to provide Plaintiffs and the Class Members with relief for the damages they suffered and will suffer.

41. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its consumers' Sensitive Information. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

42. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

43. In light of recent high profile data breaches at other healthcare partner and provider companies, Defendant knew or should have known that its electronic records and consumers' Sensitive Information would be targeted by cybercriminals.

44. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[4] The 330 reported

[4] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited June 5, 2023).

breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[5]

45. Indeed, cyberattacks against the healthcare industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[6]

46. Cyberattacks on medical systems and healthcare partner and provider companies like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[7]

47. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including M&D.

Plaintiff Facon's Experience

48. Plaintiff Facon received M&D's Breach Notice in or around March 2024.

49. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it for over eight months.

---

[5] *Id*.
[6] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited March 13, 2023).
[7] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited March 13, 2023).

50. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Sensitive Information for theft by cybercriminals and sale on the dark web.

51. Plaintiff does not recall ever learning that her Sensitive Information was compromised in a data breach incident, other than the breach at issue in this case.

52. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

53. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

54. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

55. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

56. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

57. Plaintiff suffered actual injury from the exposure and theft of her Sensitive Information—which violates her rights to privacy.

58. Indeed, following the Data Breach in March of 2024, Plaintiff's accountant informed her that Plaintiff Facon's identity was fraudulently used for tax purposes. Specifically, her accountant attempted to file Plaintiff's 2023 taxes and received an IRS notification informing them that an individual Plaintiff did not authorize had already attempted to fraudulently file Plaintiff's taxes using her identity.

59. Additionally, following the Data Breach, Plaintiff has experienced an enormous increase in spam calls and texts, suggesting that her Sensitive Information is now in the hands of cybercriminals.

60. Once an individual's Sensitive Information is for sale and access on the dark web, as Plaintiff's Sensitive Information is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[8] On information and belief, Plaintiff's phone number was compromised as a result of the Data Breach.

61. Plaintiff has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Kashvili Experience

62. Plaintiff Kashvili received M&D's Breach Notice on or around March 25, 2024.

[8] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

63. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it for over eight months.

64. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Sensitive Information for theft by cybercriminals and sale on the dark web.

65. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

66. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

67. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

68. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

69. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

70. Plaintiff suffered actual injury from the exposure and theft of his Sensitive Information—which violates his rights to privacy.

71. Plaintiff has a continuing interest in ensuring that his Sensitive Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

72. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendant.

73. As a result of Defendant's failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Sensitive Information is used;

b. The diminution in value of their Sensitive Information;

c. The compromise and continuing publication of their Sensitive Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Sensitive Information; and

h. The continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Sensitive Information in its possession.

74. Stolen Sensitive Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

75. The value of Plaintiffs' and the Class's Sensitive Information on the black market is considerable. Stolen Sensitive Information trades on the black market for years, and criminals frequently post stolen Sensitive Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

76. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

77. One such example of criminals using Sensitive Information for profit is the development of "Fullz" packages.

78. Cyber-criminals can cross-reference two sources of Sensitive Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

79. The development of "Fullz" packages means that stolen Sensitive Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other

words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Sensitive Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and the Class's stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the Data Breach.

80. Defendant disclosed the Sensitive Information of Plaintiffs and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Sensitive Information of Plaintiffs and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Sensitive Information.

81. Defendant's failure to properly notify Plaintiffs and members of the Class of the Data Breach exacerbated Plaintiffs' and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Sensitive Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

82. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Sensitive Information.

83. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of Sensitive Information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

84. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

85. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

86. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

87. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Violated HIPAA

88. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients, or in this case, consumers' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information. [9]

89. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[10]

90. The Data Breach itself resulted from a combination of inadequacies showing Defendant's failure to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

[9] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[10] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

91. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

Defendant Fails to Comply with Industry Standards

92. As noted above, experts studying cyber security routinely identify entities in possession of PII and PHI as being particularly vulnerable to cyberattacks because of the value of the Sensitive Information which they collect and maintain.

93. Several best practices have been identified that a minimum should be implemented by employers in possession of PII and PHI, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

94. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

95. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center

for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

96. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

97. Plaintiffs sue on behalf of themselves and the proposed nationwide class ("Class") and state subclass ("Subclass"), defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> **Nationwide Class:** All individuals residing in the United States whose Sensitive Information was compromised in the M&D Data Breach including all those who received notice of the breach.
>
> **New York Subclass:** All individuals residing in New York whose Sensitive Information was compromised in the M&D Data Breach including all those who received notice of the breach.

98. Excluded from the Class is Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

99. Plaintiffs reserve the right to amend the class definition.

100. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiffs are representative of the Class, consisting of several thousand members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiffs' claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's interests. Their interests do not conflict with the Class's interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

    i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's Sensitive Information;

    ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

    iii. Whether Defendant were negligent in maintaining, protecting, and securing Sensitive Information;

    iv. Whether Defendant breached contract promises to safeguard Plaintiffs' and the Class's Sensitive Information;

    v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiffs' and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

101. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

102. Plaintiffs reallege all previous paragraphs as if fully set forth below.

103. Plaintiffs and members of the Class entrusted their Sensitive Information to Defendant. Defendant owed to Plaintiffs and the Class a duty to exercise reasonable care in handling and using the Sensitive Information in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

104. Defendant owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their Sensitive Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Sensitive Information —just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality

of Plaintiffs' and the Class's Sensitive Information by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the Sensitive Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

105. Defendant owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their Sensitive Information. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and the Class to take appropriate measures to protect their Sensitive Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

106. Defendant owed these duties to Plaintiffs and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and the Class's Sensitive Information.

107. The risk that unauthorized persons would attempt to gain access to the Sensitive Information and misuse it was foreseeable. Given that Defendant holds vast amounts of Sensitive Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Sensitive Information —whether by malware or otherwise.

108. Sensitive Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Sensitive Information of Plaintiffs and the Class and the importance of exercising reasonable care in handling it.

109. Defendant breached its duties by failing to exercise reasonable care in supervising its employees, agents, contractors, vendors, and suppliers, and in handling and securing the Sensitive Information of Plaintiffs and the Class which actually and proximately caused the Data Breach and Plaintiffs' and the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

110. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Sensitive Information by criminals, improper disclosure of their Sensitive Information, lost benefit of their bargain, lost value of their Sensitive Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

111. Plaintiffs reallege all previous paragraphs as if fully set forth below.

112. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's Sensitive Information.

113. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, patients' Sensitive Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's Sensitive Information.

114. Defendant breached its duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Sensitive Information.

115. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

116. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l).

Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

117. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Sensitive Information.

118. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and the Class's Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

119. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

120. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect their PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

121. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiffs and members of the Class, Plaintiffs and members of the Class would not have been injured.

122. The injury and harm suffered by Plaintiffs and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their Sensitive Information.

123. Had Plaintiffs and the Class known that Defendant did not adequately protect their Sensitive Information, Plaintiffs and members of the Class would not have entrusted Defendant with their Sensitive Information.

124. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

125. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of Sensitive Information; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Sensitive Information, entitling them to damages in an amount to be proven at trial.

126. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their Sensitive Information, which remain in Defendant's possession and is subject to further

unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their Sensitive Information in its continued possession.

COUNT III
Breach of Contract
(On Behalf of Plaintiffs and the Class)

127. Plaintiffs reallege all previous paragraphs as if fully set forth below.

128. Defendant entered into various contracts with its clients, including healthcare providers, to provide medical billing services to its clients.

129. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiffs and the Class, as it was their confidential information that Defendant agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Sensitive Information belonging to Plaintiffs and the Class were the direct and primary objective of the contracting parties.

130. Defendant knew that if it were to breach these contracts with its healthcare provider clients, the clients' consumers, including Plaintiffs and the Class, would be harmed by, among other things, fraudulent misuse of their Sensitive Information.

131. Defendant breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiffs' and Class Members' Sensitive Information.

132. As reasonably foreseeable result of the breach, Plaintiffs and the Class were harmed by Defendant failure to use reasonable data security measures to store their Sensitive Information, including but not limited to, the actual harm through the loss of their Sensitive Information to cybercriminals.

133. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

134. Plaintiffs reallege all previous paragraphs as if fully set forth below.

135. Plaintiffs and members of the Class conferred a benefit upon Defendant in providing Sensitive Information to Defendant.

136. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and the Class. Defendant also benefited from the receipt of Plaintiffs' and the Class's Sensitive Information, as this was used to facilitate its services to Plaintiffs and the Class.

137. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Sensitive Information.

138. Instead of providing a reasonable level of security, or retention policies, which would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

139. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and the Class's Sensitive Information because Defendant failed to adequately protect their Sensitive Information.

140. Plaintiffs and Class Members have no adequate remedy at law.

141. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

142. Plaintiffs reallege all previous paragraphs as if fully set forth below.

143. Given the relationship between Defendant and Plaintiffs and Class Members, where Defendant became guardian of Plaintiffs' and Class Members' Sensitive Information, Defendant became a fiduciary by its undertaking and guardianship of the Sensitive Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Sensitive Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

144. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their Sensitive Information.

145. Because of the highly sensitive nature of the Sensitive Information, Plaintiffs and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their Sensitive Information had they known the reality of Defendant's inadequate data security practices.

146. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class Members' Sensitive Information.

147. Defendant also breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

148. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

COUNT VI
Violation Of The New York Deceptive Trade Practices Act ("GBL")
(New York Gen. Bus. Law § 349)
(On Behalf of Plaintiff Kashvili and the Class, and in the alternative, the New York Subclass)

149. Plaintiff Kashvili realleges all previous paragraphs as if fully set forth below.

150. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

a. Misrepresenting material facts to Plaintiff and the Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' Sensitive Information from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts to Plaintiff and the Class by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' Sensitive Information;

c. Omitting, suppressing, and/or concealing material facts of the inadequacy of its privacy and security protections for Class Members' Sensitive Information;

d. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class Members' Sensitive Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws; and,

e. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa (2).

151. Defendant knew or should have known that its network and data security practices were inadequate to safeguard the Class Members' Sensitive Information entrusted to it, and that risk of a data breach or theft was highly likely.

152. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security.

153. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class Members) regarding the security of Defendant's network and aggregation of Sensitive Information.

154. The representations upon which current and former patients (including Plaintiff and Class Members) relied were material representations (e.g., as to Defendant's adequate protection of Sensitive Information), and current and former patients (including Plaintiff and Class Members) relied on those representations to their detriment.

155. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead patients acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and other Class Members have been harmed, in that

they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

156. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Class Members' Sensitive Information and that the risk of a data security incident was high.

157. Defendant's acts, practices, and omissions were done in the course of Defendant's business of furnishing services to consumers in the State of New York. 167.

158. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and Class Members' Sensitive Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class Members damages.

159. Plaintiff and Class Members were injured because:

f. Plaintiff and Class Members would not have accepted Defendant's services had they known the true nature and character of Defendant's data security practices;

g. Plaintiff and Class Members would not have entrusted their Sensitive Information to Defendant in the absence of promises that Defendant would keep their information reasonably secure, and

h. Plaintiff and Class Members would not have entrusted their Sensitive Information to Defendant in the absence of the promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

160. As a direct and proximate result of Defendant's multiple, separate violations of GBL §349, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries.

The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' Sensitive Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Sensitive Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff and the proposed class entrusted Defendant with their Sensitive Information; and (h) the continued and substantial risk to Plaintiff's and Class Members' Sensitive Information, which remains in the Defendant's possession with inadequate measures to protect Plaintiff's and Class Members' Sensitive Information.

161. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

162. Plaintiff brings this action on behalf of himself and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow patients to make informed purchasing decisions and to protect Plaintiff, Class Members and the public from Defendant's unfair, deceptive, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

163. Plaintiff and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

164. On behalf of himself and other members of the Class, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover her actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

165. Also as a direct result of Defendant's violation of GBL § 349, Plaintiff and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendant to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

PRAYER FOR RELIEF

Plaintiffs and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen Sensitive Information;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

Dated: March 29, 2024

Respectfully submitted,

By: /s/ James J. Bilsborrow

James J. Bilsborrow
WEITZ & LUXENBERG, PC
700 Broadway
New York, New York 10003
Tel: (212) 558-5500
jbilsborrow@weitzlux.com

TURKE & STRAUSS LLP
Samuel J. Strauss
Raina Borrelli
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiffs and Proposed Class